International Journal of Mechanical Engineering and Technology (IJMET)
Volume 10, Issue 01, January 2019, pp. 8–24, Article ID: IJMET_10_01_002
Available online at http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=10&IType=1
ISSN Print: 0976-6340 and ISSN Online: 0976-6359

© **IAEME** Publication **Scopus** Indexed

SECURE LOCATION MAP AND ENCRYPTION KEY BASED ON INTELLIGENCE SEARCH ALGORITHM IN ENCRYPTION AND STEGANOGRAPHY TO DATA PROTECTION

Alaa Kadhim Farhan
Computer Sciences Department, University of Technology/ Iraq

Rasha Subhi Ali
Department of Computer Techniques Engineering, AL Nisour University College/ Iraq

Sura Mazin Ali
Al Mustansiriyah University/ Iraq

ABSTRACT

In the digital world, data is that the heart of computer communication and world economy to make sure the safety for this data it is desired secure transmission of confidential data that gets an excellent deal of attention. Therefore; it's necessary to use effective methods to reinforce information security. Many strategies are coming up to shield the information from going to unauthorized person. Steganography and cryptography are 2 completely different mechanisms for information security. The main purpose in cryptography is to create message idea unintelligible, whereas steganography aims to hide secret message. Digital-pictures are wonderful carriers of hidden information. Combining these two methods is a topic of high relevance since secure communication is inevitable for mankind. In this paper, a method for protection data was proposed comprises a hybridization between cryptography and steganography. In the proposed approach particle swarm optimization algorithm (PSO) was used in both methods(encryption and steganography).The PSO algorithm was used in key generation process for data encryption and in generating hidden locations for data hiding. Also, the Least Significant Bit (LSB)was utilized to add the encrypted data into LSB of the cover and the PSO was utilized to specify the location of hiding data. The data will be encrypted by using stream cipher method. The image will be transmitted and received through the internet and the extraction process would be exactly reveres for hidden process. Experimental results illustrate that the visual, and therefore applying mathematics values of the image with encrypted information before the insertion represented as the same as the values after the insertion so that the reduction in the possibility of the confidential-message to be detected and allows secret communication. The effectiveness of the projected technique has been calculable by computing 5 statistical tests, 16 NIST tests for the generated key and

encryption algorithm respectively; also, the steganography statistical tests such as Mean square error (MSE), Peak Signal to Noise Ratio (PSNR), Average Difference (AD), Maximum Difference (MD), Normalized Cross-correlation (NC), Mean Absolute Error (MAE), Normalized Absolute Error (NAE), Structural Content (SC), Signal-To-Noise Ratio(SNR), Similarity Measure (SIM) and Unified average changing intensity Measure (UACI) are computed.

Key words: Least Significant Bit (LSB), Stream Cipher Method, Particle Swarm Optimization method, Steganography.

Cite this Article: Alaa Kadhim Farhan, Rasha Subhi Ali, Sura Mazin Ali, Secure Location Map and Encryption Key Based on Intelligence Search Algorithm in Encryption and Steganography to Data Protection, *International Journal of Mechanical Engineering and Technology* 10(1), 2019, pp. 8–24. http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=10&IType=1

1. INTRODUCTION

Data security has become a big resource nowadays for the effective operations of the various demands of any organization. One among the most necessary demands from those networks is to supply secure data transmission from one position to a different. Cryptography is one among the mechanisms that give most secure way to transfer the sensitive information from sender to supposed receiver. Its major aim is to create sensitive information unreadable to all un authorized users except the supposed receiver [1]. Cryptography is one of the main categories of computer security. In Cryptography the original-message is transformed into non-readable message. That is cryptography hides information from prying eyes. Encryption algorithms are of two types asymmetric and symmetric. Asymmetric encryption algorithms are almost 1000 times slower than symmetric encryption algorithms, because they require more computational processing power. So symmetric encryption algorithms are commonly used now days; but cryptography isn't able to hide the presenting of data alone and it can't protect data effectively. Any eavesdropper can easily detect the presence of encrypted data and can try several attacks in order to get the original data. So that to enhance the security there is a need to provide two-layer approach for providing an improved and better security. Steganography is concerned with security of transmitting data and allows communicating secretly by hiding the data within data (text/image) [2]. Steganography is the process of hiding the presence of a secret-message, so that no one will see the hiding message. Table1 shows a comparison of varied techniques for communicating in secret [3].

Table 1 Comparison of Secret Communication Techniques [5]

Secret-Communication-Technique	Confidentiality	Integrity	Unremovability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

The following is a list of main requirements that steganography techniques must satisfy [3]:

a) The integrity of the hidden information after it has been embedded inside the stego object must be correct..

b) The stego object must remain unchanged or almost unchanged to the naked eye.

c) In watermarking, changes in the stego object must have no effect on the watermark.

d) Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively [4].

2. CRYPTOGRAPHY

Cryptography is the science of mistreatment arithmetic to cipher and decipher information to stay messages secured by remodeling intelligible information form (plaintext) into unintelligible kind (cipher text) [6].The basic idea for cryptography is: at sender-side plaintext is converted into cipher text by using encryption algorithms; Cipher text is transmitted over the transmission-medium and it was reached to the receiver, and at receiver-side cipher ext is converted back to the original plaintext by utilizing decryption algorithm. Figure1 shows this idea behind cryptography [7].

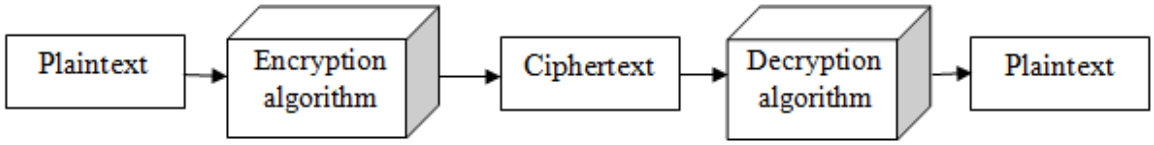


Figure 1 Encryption and decryption Process [7]

3. IMAGE STEGANOGRAPHY

Image Steganography is the art of hiding secret messages into a digital image. This method exploits the failure of the Human-Visual-System (HVS).The HVS cannot detect the difference in luminance of color vectors in pixels color set. Forexample:a24-bit picture can have 8bits, representing every 3 color-values (red, green, and blue) in every pixel. If there is a tendency to take into account just the blue there'll be two totally different values of blue. The distinction between11111111and11111110within the value of blue intensity is probably going to be undetectable by the human eye. Hence; if the terminal recipient of data was nothing however human the least(HVS) then the Least-Significant-Bit(LSB) are often utilized for one thing else excluding color information. The LSB technique was used to hiding information within a picture file [8].There are 4 different types of steganography such as Text steganography, Audio/Video steganography, Image steganography. Image-steganography represents the most widely used method for hiding data. Because it is a quite simple and secure method for transferring data over the internet [2].

The LSB is that the lowest bit in an exceedingly series of numbers in binary E.g. within the binary number:10110001, the LSB is much right one. The LSB primarily based Steganography is one in all the steganography strategies, utilized to embed the key information into the LSB of the pixel values in an exceedingly cover [9].LSB for the patching of data is used because the intensity of image is only changed by 1 or 0 after hiding the information. The change is only one bit so that the intensity of image is not affected too much and we can easily transfer the data. This results in LSB is most efficient (in term of data hiding) method of image steganography [2].

PIXELS: 00100110 11101001 11001001

00100110 11001001 11101000

11001001 00100110 11101000

241 : 011110001

RESULT: 00100110 11101001 11001001

00100111 11001001 11101000

11001000 00100111 11101000

Here the number240is embedded into first eight bytes of the grid and only 6 bits are changed.

4. PARTICLE SWARM OPTIMIZATION ALGORITHM

Swarm Intelligence (SI) describes the evolving collective intelligence of population/groups of autonomous agents with a low level of intelligence. Particle Swarm Optimization (PSO) is an evolutionary algorithm inspired by animal social behavior. PSO achieves performance by iteratively directing its particles toward the optimum using its social and cognitive components [10].PSO could be a robust random optimization technique supported the movement and intelligence of swarms. PSO applies the conception of social interaction to downside determination. it absolutely was developed in 1995 by James Kennedy (social-sychologist) and Russell Eberhart[11].PSO achieves performance by, iteratively leading its particles toward the optimum utilizing social and psychological feature parts. Locations of particles; denoted by(xi,j), are influenced by their velocity element at intervals then-dimensional search area, denoted by(Vi,j), wherever(i) represents the particle's index and j is that the dimension at intervals the search area. In PSO; particles are thought of to be potential solutions, they fly through the virtual space with relevance most rate limitations; denoted by(Vmax). Particles are typically interested in the Positions that yield the simplest results. The simplest positions, as an example local_best (pi,j) and international best (gi), are keep in every particle's Memory. In general; the local_best from every particle is seen as a result of the position during that the particle achieved its highest-performance; where versa the global-best of every particle is seen as a result of the most effective local-best location achieved by neighbor particles [10]..After finding the 2 best values every particle updates its velocity (vi, j) and position(Pi, j) towards its Pbest and gbest-locations as follows:

Particle-Velocity-Update [11]:

$$\boldsymbol{vi,j = covi,j + c1r1(Ppbesti,j - pi,j) + c2r2(Pgbesti,j - Pi,j}$$

Particle-Position-Update:

$$\boldsymbol{Pi,j = Pi,j + vi,j}$$

Where; Ppbesti;(j) and Pgbesti;(j) are the particle-best and global-best position of the particles sequentially. PSO an attractive optimization technique. By varied these factors, it's potential to use PSO in a very wide range of applications [11].

5. DESIGN AND IMPLEMENTATION

In this paper a proposed technique comprising a combination of cryptography and steganography to solve the problem of unauthorized data access. Steganography can be applied to hide encrypted or plain data; so it increases the security of this data. In the proposed method the message was encrypted in the first stage by using stream cipher method and PSO algorithm. Symmetric stream cipher algorithm because the encryption key decryption key, plaintext, cipher text and internal operation in the encryption or decryption process is based on the integer numbers. The plaintext size for encryption process is dynamic not specific. The PSO algorithm was used to create different numbers which can be used as locations for hiding data in the images, in this points the PSO algorithm enhanced the steganographic systems by generating secret locations depending on the user secret key. LSB steganography technique was used to hide the encrypted data in each color of the generated

locations. Secrets can be hidden in all forms of cover info. The following formula provides a very generic description of the steganographic process:
cover_medium + hidden_data + secret map = stego_medium

In this context, the cover_medium means that the file in that the hidden data are going to be hidden. The resultant file is that the stego_medium (which can be identical kind of file as the cover_medium). There are four ways that to implement steganography using (text; images; audio files or video files).For security, most effective encryption might not be enough; as a result the proposal consists of Steganography with encryption process are used to increase data protection. The content of message appears meaningless to the third party, so it is very difficult to detect the hidden message. The combination of the steganography with encryption techniques will enhance the security of embedded data and will be satisfied the requirements such as security, robustness and capacity for secure data transmission over an open channel. So that if the attacker was defeat the stenographic method to detect the message from stego-image, then he/she would still need the cryptographic method to decipher the encrypted message. The image will be transmitted and received through the internet, the receiver will extract the hidden data from the image and decrypt it to retrieve the original data with the image. The proposed method explained in figure2.

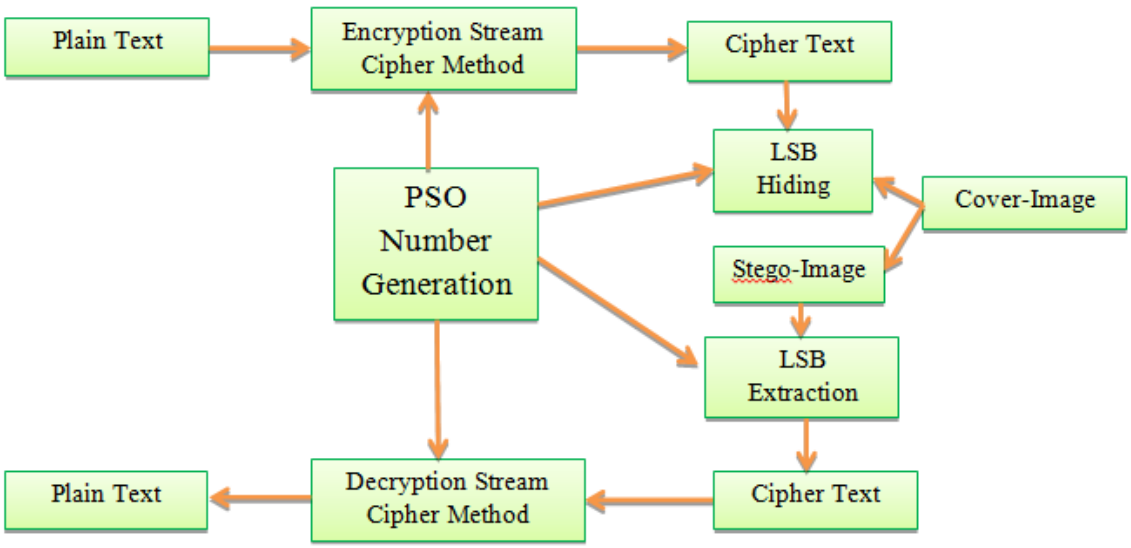


Figure 2 The Proposed Method

1. Key generation process: PSO artificial intelligence method was used in generating random numbers which are used in hiding locations and as keys used in the encryption and decryption process. These numbers generated by using secret key utilized in sender and receiver site, from this key 256 different values of double hexa items are generated. Each number from these items represent the axis points for (X and Y); first one for X-Axis and the second one for Y-Axis. The key generation process explained in algorithm1 with an example for each step.

Algorithm1: Key Generation

Input: secret key

Output: 256 different double values of hexa formation.

Begin:

Step1: Calculate ascii code of secret key characters let it be a.

Step2: Calculate length of secret key let it be b.
Step3: If b<16 then padding a by adding zeroes.
Step4: Do step 5 to 7 if i=0
Step5: Calculate x(i)
x(i) =asc(a(i))
Step6: Calculate y1(i) and y2(i).
Y1(i)=(i mod b)/b
Y2(i)=((i*2) mod b)/(b+i)
// Where x(i) and y(i) represent particle position //
Step7: Calculate velocity values let it be v(i).

```
v(i) = Round(((y1(i) + y2(i)) * Asc(a(i)) Mod 255).
Step8: Do step 9 to 10for creation 255 times let i=2
```

Step9: Calculate global best positions let it be g
If i<= 15 Then
g = Asc(Mid(a, i, 1)) Mod 256
Else
g = (Asc(Mid(a, (i Mod b) + 1, 1)) Xori) Mod 256
End If
Step10: Compute new velocity values
y1(i - 1) = (i Mod b) / b // i-1=1 means the values will be saved in locations 1 to 255 //
y2(i - 1) = ((i * 2) Mod b) / (b + i)
v(i - 1) = Round(((v(i - 2) + y1(i - 1) * (i - x(i - 2)) + y2(i - 1) * (g - x(i - 2))) + i) Mod 256)
x(i - 1) = (v(i - 1) + x(i - 2)) Mod 256.
End

Example2 about key generation let
Secret Key=ABC
Length(ABC)=3
A="ABC0000000000000"
X(0)=65
Y1(0)= 0.33333333333333331
Y2(0)= 0.5
V(0)= 54
Calculate g
G=66
Y1(1)= 0.66666666666666663
Y2(1)= 0.2
X(1)= 79
V(1)= 14

These steps9 to 10 in algorithm1 calculated for 255 times

The generated key Velocity values in hexa=

9AF973DEFE0590FF3B13A8A1792D020ACBCF0B7E248D151CF02BAC85181A3E20
EE2223D3F1D98225C88836A92627333211C3430729B7CD2A516A2F37383AAD5AF400
F63C3D41BF4704149D494BBD4D014E505355570D3431E8A359C15B5CBA5E031EF7C
A3F60F36269E3A46C8AAAB893946D6E866F7276B3CE74755677AB7B7C8384B087EB3

0898BDD085416928C1017808E91217870962C48F59798D1399C1BD29E9FA5A64699A71
94AAFB1BBE4AEBE4CC4C966CCD0B22ED5D6ED8128D7719B52DADCB9677FDFE00
6C2630E65C6E1B4E2D4B6A2E5E668B57DE9DB12EAEC581F955FEFF2C7F8356109FA
420C5DA0458FFBFCC5BCE76B4FFD64447A0F40D81DC0

The generated locations Velocity values in hexa=

9A	F9	73	DE	FE	05	90	FF	3B	13	A8	A1	79	2D	02	0A
CB	CF	0B	7E	24	8D	15	1C	F0	2B	AC	85	18	1A	3E	20
EE	22	23	D3	F1	D9	82	25	C8	88	36	A9	26	27	33	32
11	C3	43	07	29	B7	CD	2A	51	6A	2F	37	38	3A	AD	5A
F4	00	F6	3C	3D	41	BF	47	04	14	9D	49	4B	BD	4D	01
4E	50	53	55	57	0D	34	31	E8	A3	59	C1	5B	5C	BA	5E
03	1E	F7	CA	3F	60	F3	62	69	E3	A4	6C	8A	AA	B8	93
94	6D	6E	86	6F	72	76	B3	CE	74	75	56	77	AB	7B	7C
83	84	B0	87	EB	30	89	8B	DD	08	54	16	92	8C	10	17
80	8E	91	21	78	70	96	2C	48	F5	97	98	D1	39	9C	1B
D2	9E	9F	A5	A6	46	99	A7	19	4A	AF	B1	BB	E4	AE	BE
4C	C4	C9	66	CC	D0	B2	2E	D5	D6	ED	81	28	D7	71	9B
52	DA	DC	B9	67	7F	DF	E0	06	C2	63	0E	65	C6	E1	B4
E2	D4	B6	A2	E5	E6	68	B5	7D	E9	DB	12	EA	EC	58	1F
95	5F	EF	F2	C7	F8	35	61	09	FA	42	0C	5D	A0	45	8F
FB	FC	C5	BC	E7	6B	4F	FD	64	44	7A	0F	40	D8	1D	C0

2. Encryption process: The stream cipher algorithm was used for the encryption process, the XOR operation between the Asci code for plain text characters and Asci code for generating keys characters are used for encrypting the plain message. The secret message size is checked such that the size of the secret message should be less than the size cover image. The PSO generated keys should be same on both sides (sender and receiver sides). The steps of encryption process are explained in figure3 and figure4 with an example.

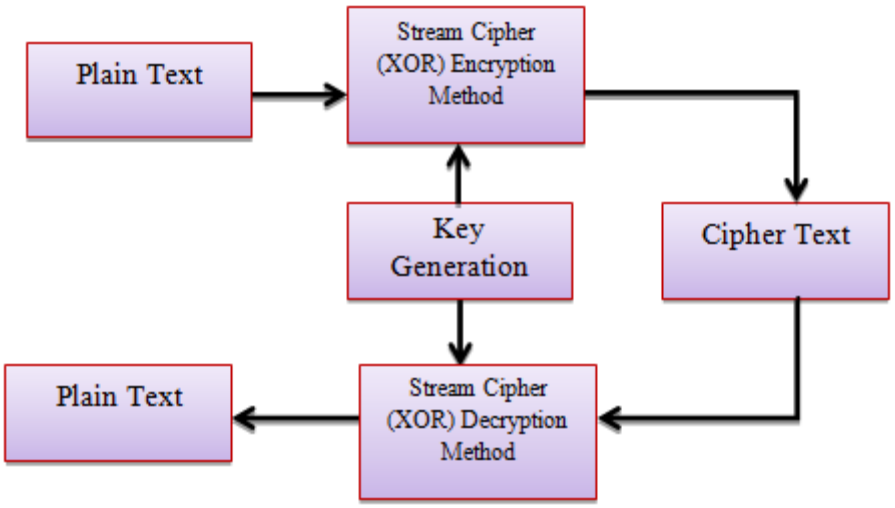


Figure 3 Encryption and Decryption Process

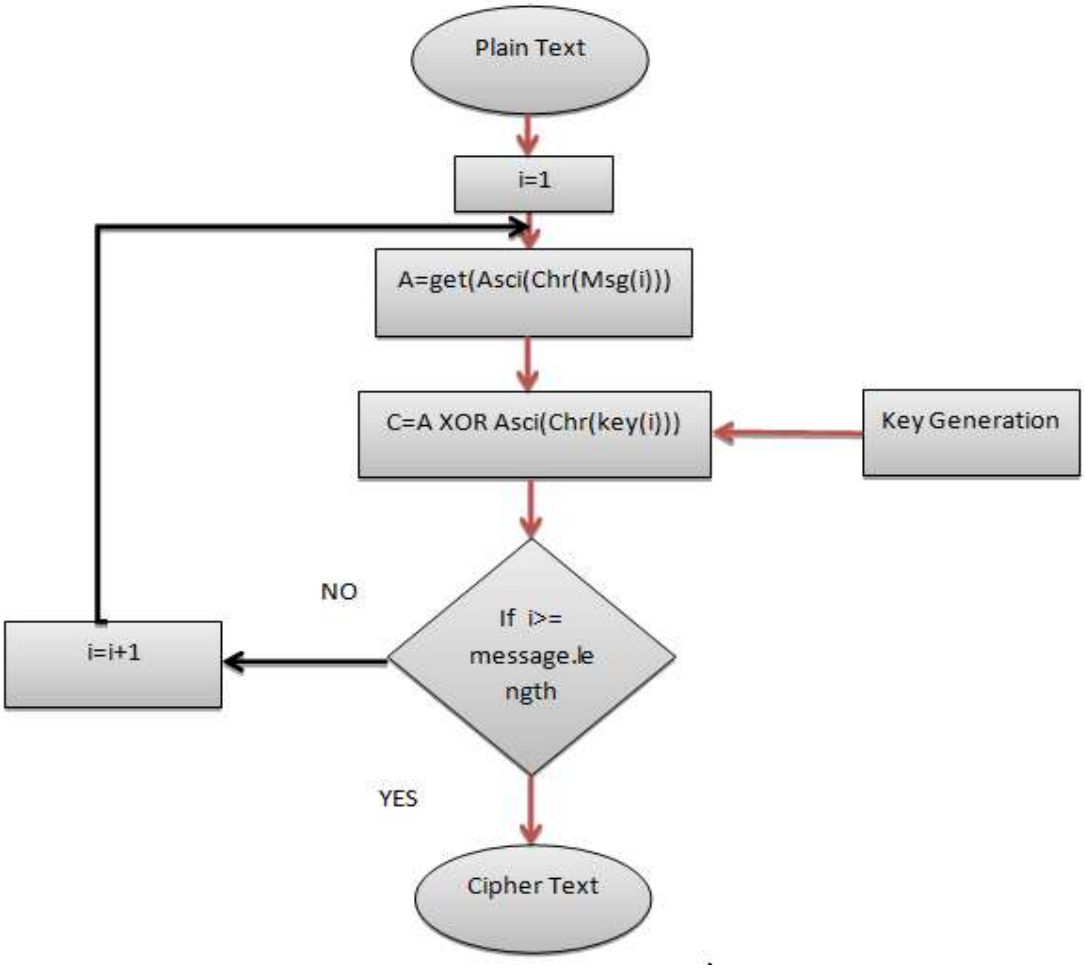


Figure 4 Stream Cipher Encryption Process

Example3 about Encryption Process let

PlainMessage=Security

Let i=1

Character (i)=S

Cipher+=Chr (Asci(S)XOR Asci(9)= "ↄ"

I=i+1=2

Cipher+=Chr(Asci(e)XOR Asci(A))= "ↄ\"

This process ending until last message character is reached

Cipher= "ↄ\TF6,2<"

3. Steganography process: this concept includes reading the cover image data, secret locations generated by using algorithm1 and secret message. After that each character of secret message is converted to binary data, if the length of binary data less than 8 bits the padding it left by0's. Each character of the secret message will be hiding in 3 pixels. In this work the LSB method will be used for hiding data. The steps for hiding and retrieving data are illustrated in the algorithm (2 and 3):

Algorithm2: hide text message:

Input: Cover image, Secret message.

Output: Stego_image.

Begin:

Step 1: Read the cover image and secret message which is to be hidden in the cover image.

Step 2: Generate hiding locations by using PSO algorithm let it be L.

Hiding locations= message length*3 e.g. if message length= 3 characters, then hiding locations=3*3=9

Step3:Split L to 256 cells of double values. // X=First value and Y=Second value e.g the location(i)="9A"; X=Ascii(9) and y=Ascii(A) //

Step3: Read secret message and write the length in first location in the cover image. In example 2 first location="9A"

Step4: For each character in the secret message do

Step5: Convert the character to binary form.

Step6: For each character read three locations from the generated array of algorithm1, these locations include the pixel position in the cover image.

Step7: Calculate LSB of each pixel in the array cells generated by using PSO algorithm of cover image.

Step 8: Replace LSB of the cover image with each bit of secret message one by one.

Step 9: Write stego image.

End.

The process of hiding by using LSB method includes:

1- Convert characters of the Secret Message to binary

2- Hide each character in 3 pixels in LSB of RGB values

3- Write the result to the Stego_image

4- This process continued until all secret message characters are hidden

Algorithm3 to retrieve text message:-

Input: Stego_image image, Secret Key.

Output: Plain message.

Begin:

Step 1: Read the stego image.

Step2: Generate hiding locations by using PSO algorithm let it be L.

Step3:Split L to 256 cells of double values.

Step4: Extract the length of message from the first cell of array generated by using algorithm1 // the first cell in example2 = "9A" then X=First value and Y=Second value e.g the location(i)="9A"; X=Ascii(9) and y=Ascii(A); length= value stored in pixel(54,65) =8//

Hiding locations= message length*3 e.g. message length= 8 characters, then hiding locations=3*8=24

Step5: From each location in the generated array calculates LSB of each pixel of stego image.

Step6: For getting one byte repeat step 4 for 8 locations.

Step7: Retrieve bits and convert each 8 bits into a character.

Step8: Repeat step 5 to 7 until achieving maximum length of the message.

End.

The main steps for hiding and extracting data are summarized in the following steps:

Firstly an image is read from the computer; generate 3 locations for each character and then convert the character and RGB values of the extracted location to binary form. After that, the message characters are embedded using the LSB method for each character 3 pixels were needed. Next, writing the results of substitution into the stego_image, then hide the message length into image cover in pixel of first generated key values in Red Value. Finally the extraction process, this process includes extracting the length of the secret message and secret message which was embedded during the embedding process in the first step. At first declare message bytes by reading a pixel location from the locations generated by using PSO algorithm starting from the second location (for extracting one byte we need to read 3 locations). Extract the LSB bits and put it in k, when k =8, a byte is extracted. Repeat for extracting next byte.

6. ANALYSIS & RESULTS

The performance of the proposed merged methods is evaluated by measuring key statistical analysis, metrics for Picture Quality Evaluation and 16 NIST tests. In this work, vb.net is implemented for processing the proposed system. In order to demonstrate the online transmission of hidden data by using the proposed system. At the sender side, it is required to provide original image, PSO algorithm, secret key, DNA table coding and secret message to be hiding in the stego_image. At the receiver side, it is required to provide stego_image, PSO algorithm, secret key, retrieving the encrypted message and finally decrypting the retrieved message to get the plain text.

The analysis and results of this work illustrated in five measures:

1- Time space

2- Complexity

3- Statistical test for generating key algorithm and the encryption algorithm

4- Brute force attack

5- Steganography Statistical tests: these tests include several parameters like MSE, PSNR, AD, MDR, MDG, MDB, NC, MAE, NAE, SC, SNR, UACI and SIM. The values for these parameters are shown in table 4, and

6.1. Time space

This measurement involved the consumed time for encryption, decryption, hiding and retrieving messages. The consumed time was measured in milliseconds and it was shown in table 2.

Table 2 Time consuming for encryption_hidding data and decryption_retrieving data

File name	File size	File Type	Length of secret msg	E+S time	D+S time	Horizontal Resolution		Vertical Resolution	
						Original-Image	Stego-Image	Original-Image	Stego-Image
images	1.12 k	Jpg	47	0.279	0.599	96 dpi	96 dpi	96 dpi	96 dpi
download (4)	2.16 k	Jpg	13	0.03	0.055	96 dpi	96 dpi	96 dpi	96 dpi
download (3)	10.4 k	Jpg	28	0.059	0.115	96 dpi	96 dpi	96 dpi	96 dpi
download (1)	4.19 k	Jpg	39	0.084	0.16	96 dpi	96 dpi	96 dpi	96 dpi
images (1)	16.7 k	Jpg	43	0.095	0.172	96 dpi	96 dpi	96 dpi	96 dpi
download (2)	4.33 k	Jpg	48	0.101	0.192	96 dpi	96 dpi	96 dpi	96 dpi
download (2)	4.33 k	Jpg	46	0.095	0.192	96 dpi	96 dpi	96 dpi	96 dpi
images (1)NEW	11.8 k	Jpg	51	0.101	0.2	96 dpi	96 dpi	96 dpi	96 dpi
imagesGIF	27 K	Gif	38	0.09	0.163	242 dpi	242 dpi	208 dpi	208 dpi

imagesbmps	147 k	Bmp	38	0.077	0.156	242 dpi	242 dpi	208 dpi	208 dpi
imagesPNG	136 k	Png	38	0.081	0.165	242 dpi	242 dpi	208 dpi	208 dpi
Lenna_Original	78.6 k	Png	46	0.093	0.191	200 dpi	200 dpi	200 dpi	200 dpi

E+S time=consumed time for Encryption and Steganography process

D+S time=consumed time for Decryption and Retrieval message process

From table 2, it is noted that the proposed algorithm consumed too small amount of time for encryption, hiding data, decryption, and retrieving messages. The time taken does not exceed a second.

6.2. Complexity

For the proposed method to be broken the attacker needs to know the utilized algorithm, secret key, length of key, length of encrypted message, secret maps for generating hiding locations, location of hiding message length, which color value the length of message was embedded, key generation algorithm and finally there is important thing needs to know the secure lock up table which is shared between the sender and receiver, these seven objects are increased the complexity of the proposed method. So, if the attacker gains one of these requirements, then it was remaining needs another eight things to gain the plain message. The strength of the proposed method depended on this nine points.

6.3. Statistical tests for generating key and Encryption Method

In this work the generated keys are tested by using five statistical tests (FREQUENCY TEST, RUN TEST (T0 AND T1), POKER TEST, SERIAL TEST and **AUTO_CORRELATION TEST**). The generated key was depended on utilized secret key of the receiver, so that the generated keys varying from user to another and the length of generating key equal 512 characters. The tests are shown in table3 and it was noted the algorithm for key generation has high strength; because of it was passed a proximity all five tests. Also, the tests for the encryption algorithm were shown in table 4 and it was passed most of the 14 NIST tests.

Table 3 Five Statistical Tests for the Generated Key

Secret Key	FREQUENCY TEST	RUN TEST T0	RUN TEST T1	POKER TEST	SERIAL TEST	AUTO_CORRELATION TEST
ABC ABC	PASS	PASS	PASS	PASS	PASS	PASS
ASD ASD	PASS	FAIL	PASS	PASS	PASS	PASS
Asdasd	PASS	FAIL	PASS	PASS	PASS	PASS
computer science	PASS	PASS	PASS	PASS	PASS	PASS
data security	PASS	FAIL	PASS	PASS	PASS	PASS
Data Security	PASS	PASS	PASS	PASS	PASS	PASS
mohammed 1990	PASS	PASS	FAIL	PASS	PASS	PASS
علي احمد	PASS	FAIL	PASS	PASS	PASS	PASS

Table 4 NIST Statistical Tests for the Encryption Algorithm

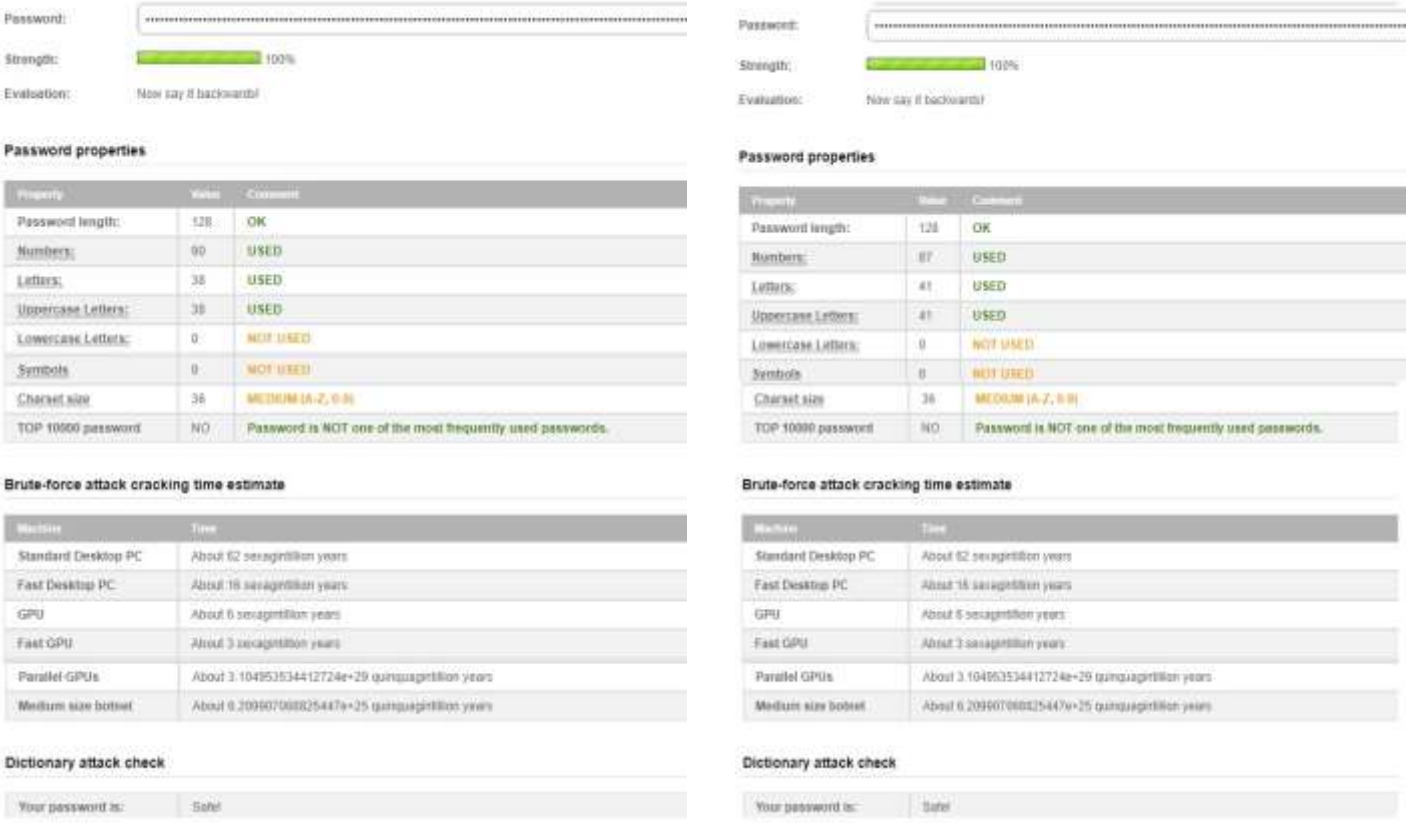
	Statistical Tests	**XOR Proportion**
Test 1	Freq	0.9967
	BlkFreq	0.9933
	CuSum	0.9933
	CuSum	0.9933
	Runs	1.0000
	Long-Run	1.0000
	Rank	0.0000
	Fft	1.0000
	Nonperiodic	0.9500
	Overlapping	1.0000
	Universal	1.0000
	Apen	1.0000
	Serial	0.9633
	Serial	0.9800
	LempelZiv	1.0000
	LinComp	1.0000
Test 2	Freq	0.9967
	BlkFreq	0.9933
	CuSum	0.9933
	CuSum	0.9933
	Runs	1.0000
	Long-Run	1.0000
	Rank	0.0000
	Fft	1.0000
	Nonperiodic	0.9567
	Overlapping	1.0000
	Universal	1.0000
	Apen	1.0000
	Serial	0.9633
	Serial	0.9800
	LempelZiv	1.0000
	LinCom	1.0000
Test 3	Freq	0.9870
	BlkFreq	0.9800
	CuSum	0.9850
	CuSum	0.9880
	Runs	0.9900
	Long-Run	1.0000
	Rank	1.0000
	Fft	1.0000
	Nonperiodic	0.9780
	Overlapping	1.0000
	Universal	1.0000
	Apen	0.1450
	Serial	0.9110
	Serial	0.9680
	LempelZiv	1.0000
	LinComp	0.0000
Test 4	Freq	0.9890
	BlkFreq	0.9830
	CuSum	0.9885
	CuSum	0.9900
	Runs	0.9915
	Long-Run	1.0000
	Rank	1.0000
	Fft	0.9995

	Nonperiodic	0.9760
	Overlapping	1.0000
	Universal	1.0000
	Apen	0.1495
	Serial	0.9265
	Serial	0.9775
	LempelZiv	0.0000
	LinComp	0.0000
Test 5	Freq	0.9870
	BlkFreq	0.9780
	CuSum	0.9860
	CuSum	0.9890
	Runs	0.9900
	Long-Run	1.0000
	Rank	0.9790
	Fft	0.9990
	Nonperiodic	0.9950
	Overlapping	0.9810
	Universal	1.0000
	Apen	0.1730
	Serial	0.9240
	Serial	0.9810
	LempelZiv	1.0000
	LinComp	0.0000

6.4. Brute force attack

In cryptography, a brute force attack consists of an attacker trying many keys generated from password with a hope of guessing pthe correct key. The attacker checks all possible keys until the correct one is guessed. The following reportfor testing three keys generated by using PSO algorithm showing that the generated key using the proposed method cannot be broken by using brute force attack.

Report: brute force attack tests for passwords of length 10, 11 and 8 characters respectively.



6.5. Steganography Statistical tests

The proposed method was applied on images, these images differ in their sizes, and hidden data also differ in their sizes. The hidden data composed Arabic characters, English (capital and small letters), symbols and numerical data. The results of Steganography Statistical tests are shown in table 5,it is noted the proposed method produced a good result, there is slightly different even when hiding large amounts of data; the similarity between the original image and stego_image a proximity more than 99 %, it is clear in table 5. The comparison between some tested original images and it's stego_images are presented in figure 5, and this is shown that there are universal changes (nobody can see the hidden data) between the original and stego_images. The UACI measures the average intensity of differences between the plain image and stego_image or ciphered image, the result of UACI for ciphered image should be between 32 and 33 but for stego_image should be nearing to zeroes and this is presented in table 5; it was very near for zeroes. PSNR for steganography should be increased, the best results when the PSNR value is high. While the PSNR for ciphered image should be decreased. Also, another measurement the MSE, for steganography this measurement should be decreased and this was shown in table 5; but the MSE for ciphered image should be increased. The UACI measures the encryption Quality of the encrypted image means the changing rate for the ciphering image, and while it is here nearing to zero this means there is no changing in the original image.

Table 5 Result of Statistical Tests for theProposed SteganographyMethod

File name	File size	File Type	Length of secret msg	MSE	PSNR	AD	MDr	MDg	MDb	NC	MAE	NAE	SC	SNR	UACI	EQ	SIM %
images	1.12 k	Jpg	47	0.004	95.65	0.004	1	1	1	0	0.004	2.57	1	75.88	0.001	0.003	99.8
download (4)	2.16 k	Jpg	13	0.01	77.36	0.01	1	1	1	0	0.01	1.69	1	57.69	0.004	0.009	99.5
download (3)	10.4 k	Jpg	28	0.002	99.74	0.002	1	1	1	0	0.002	6.42	1	71.92	0.001	0.002	99.9

download (1)	4.19 k	Jpg	39	0.007	90.5	0.007	1	1	1	0	0.007	5.77	1	72.38	0.002	0.002	99.9
images (1)	16.7 k	Jpg	43	0.003	97.34	0.003	1	1	1	0	0.003	6.13	1	72.12	0.001	0.002	99.8
download (2)	4.33 k	Jpg	48	0.01	87.89	0.01	1	1	1	0	0.01	4	1	63.98	0.004	0.003	99.7
download (2)	4.33 k	Jpg	46	0.009	88.64	0.009	1	1	1	0	0.009	3.6	1	64.34	0.003	0.003	99.7
images (1)NEW	11.8 k	Jpg	51	0.004	95.77	0.004	1	1	1	0	0.004	2.6	1	75.8	0.001	0.003	99.8
imagesGIF	27 K	Gif	38	0.003	96.78	0.003	1	1	1	0	0.003	5.4	1	72.68	0.001	0.002	99.8
imagesbmps	147 k	Bmp	38	0.003	97.2	0.003	1	1	1	0	0.003	5.1	1	72.93	0.001	0.002	99.8
imagesPNG	136 k	Png	38	0.003	96.78	0.003	1	1	1	0	0.003	5.4	1	72.68	0.001	0.002	99.8
Lenna_Original	78.6 k	Png	46	0.005	94.1	0.005	1	1	1	0	0.005	1.4	1	68.57	0.001	0.003	99.7

a. Original image b. Stego_Image

Figure 5 Comparison between Original Image and Stego_Image (A And B)

6.6. Histogram Test

A histogram is used to present the distribution of characters in a message or text file. The histograms for the colors of the original images and Stego-images are illustrated in table 6. It was noted that the values of RGB color for both images (original and Stego-Images) are equal means the proposed method achieves good results.

Table 6 Histogram Values for Original and Stego-Image

original image				**Stego-Image**			
Image Name	red	green	blue	Image Name	red	green	blue
Images	31%	31%	38%	Images1	31%	31%	38%

Download (4)	33%	33%	33%	Download(4)1	33%	33%	33%
Download (3)	21%	37%	42%	Download(3)1	21%	37%	42%
Download (1)	38%	33%	29%	Download(1)1	38%	33%	29%
Images (1)	31%	31%	38%	Images (1)1	31%	31%	38%
Download (2)	47%	32%	21%	Download(2)1	47%	32%	21%
Images (1)NEW	36%	33%	31%	Images(1)NEW1	36%	33%	31%
Imagesgif	34%	35%	32%	Imagesgif1	34%	35%	32%
Imagesbmps	34%	35%	32%	Imagesbmps1	34%	35%	32%
Imagespng	34%	35%	32%	Imagespng1	34%	35%	32%
Lenaoriginal	47%	26%	27%	Lenaoriginal1	47%	26%	27%

7. CONCLUSIONS

This paper proposes a hybridize system in which a Steganography and a cryptography are used as integrated part along with newly developed enhanced security module. The design using Stream cipher algorithm for encryption, LSB technique for steganography and PSO algorithm for creation keys and hiding locations. In data hiding part the LSB steganography algorithm was used and in cryptography part the XOR stream cipher algorithm was used. The LSB primarily based steganography imbed information within the LSB of digital pictures. The LSB insertion may be a common and straightforward approach for embedding info into cover file. This paper provides effective steganography technique, so that the person can detect the variety of choosing the method to protect the information. In Image Domain, we tend to mention the foremost powerful technique referred to as LSB to hide information specially within images in any format (BMP, JPG, PNG and….etc).and in the cryptography domain the proposed algorithm achieves pass most statistical tests for key generation and encryption methods. In spite of the JPG image format is loosely image compression technique and LSB replacement do not work directly in special domain without additional processing, but here in this research work well and there is no losing in the data because of the system depended on reading all image pixels and then hiding data in the generated locations and finally saving these pixels to new images (stego-image) this represents additional process for hiding data. The proposed method takes few milliseconds for encryption and steganography processes. Also, the statistical tests show the proposed method achieves good results. The results of similarity measure proximity 99.8 %, so the hiding data cannot be detected without knowing (the utilized algorithm, secret key, length of encrypted message, algorithm for generating hiding locations, location of hiding message length, which color value the length of message was embedded, key generation algorithm and finally there is important thing needs to know the secure lock up table which is shared between the sender and receiver). The work implemented in this work can be summarized in the following:

- A new system was presented in this work, this system accomplished cryptography and steganography by using PSO algorithm for generating 256 locations and key of 512 characters. The stream cipher algorithm has been used to encrypt the secret message and then LSB hiding method was used for steganography method. Therefore, two levels of security have been provided using the proposed hybrid technique
- Steganography combined with cryptography is a powerful tool as shown in achieved results, which is enabling people to communicate without possible eavesdroppers; the proposed method provides acceptable image quality with a few distortion in the image.
- It clear to notice the statistical properties of original and Stego-Images are completely equal as shown in table 6.

REFERENCES

[1] Kadhim F, Majeed G, Ali R. , "Enhancement CAST Block Algorithm to Encrypt Big Data", In New *Trends in Information & Communications Technology Applications (NTICT)*, Annual Conference, 13 July 2017, Publisher: IEEE, DOI: 10.1109/NTICT.2017.7976119.

[2] Arati A. Pujari, SunitaS.Shinde, "Data Security using Cryptography and Steganography", *IOSR Journal of Computer Engineering (IOSR-JCE),* e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 130-139,www.iosrjournals.org, DOI: 10.9790/0661-180405130139.

[3] Pardhi A. and Joshi R., " Secure Image Steganography using DNA sequence based on DNA Cryptography", *4th International Conference on Latest Innovations in Science, Engineering and Management, ICLISEM-17*, ISBN:978-93-86171-51-1, 1st July 2017.

[4] Channalli S. and Jadhav A., "Steganography An Art of Hiding Data ", *International Journal on Computer Science and Engineering.*Vol.1 (3), 2009, 137-141, ISSN : 0975-3397.

[5] R.Nivedhitha, T.Meyyappan, and M.Phil, "Image Security Using Steganography And Cryptographic Techniques", *International Journal of Engineering Trends and Technology*, Volume3, Issue3- 2012, ISSN: 2231-5381,http://www.internationaljournalssrg.org.

[6] Marwa E. Saleh, Abdelmageid A. Aly and Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 6, 2016.

[7] William S., "Cryptography And Network Security Principles And Practice", Fifth Edition, Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall, ISBN 0-13-03221-0.

[8] Doshi R., Jain P. and Gupta L., "Steganography and Its Applications in Security ", *International Journal of Modern Engineering Research (IJMER)* www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.

[9] Walia E., Jain P. and Navdeep, "An Analysis of LSB & DCT based Steganography", *Global Journal of Computer Science and Technology*, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[10] A. Adhamand S. Sepide, "Particle Swarm Optimization: A Survey", Applications of Swarm Intelligence, Publisher: Nova Science Publishers Inc, pp.167 -179, 2011.

[11] Pandey S. and Mishra M., "Particle Swarm Optimization in Cryptanalysis of DES", International *Journal of Advanced Research in Computer Engineering & Technology*, Volume 1, Issue 4, June 2012, ISSN: 2278 – 1323.